

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-110491

(43)Date of publication of application : 23.04.1990

(51)Int.Cl.

G09C 1/10
G06F 12/14

(21)Application number : 63-264940

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 19.10.1988

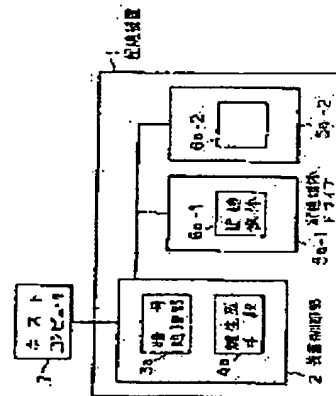
(72)Inventor : MIYAGUCHI SHOJI
IWATA MASAHIKO

(54) STORAGE DEVICE

(57)Abstract:

PURPOSE: To use different keys to each storing medium FDi and to improve the security of a storage device by storing identifying names on a recording medium and deciding the keys by using secret parameters.

CONSTITUTION: This storage device 1 is constituted of recording medium drives 51-1 and 5a-2 and a device controlling section 2. Plural recording media 6a-1 and 6a-2 are represented as FDi (i=1, 2,...) which respectively have and store identifying names IDi and protective codes Gi. Then keys Ki used for ciphering and deciphering data stored on the recording media 6a-1 and 6a-2 are fixed as $K_i = F(SG_i, ID_i)$. The SG_i is $SG_i = f_x \& Agr$, (SG_i), the F , f_x , and S of which respectively represent the key preparing algorithm held by the storage device, internal function of the F , and secret parameter of the F . Therefore, individual keys can be used for the storing media 6a-1 and 6a-2 without using any key management file and the storing content of the storage device can be ciphered and deciphered.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

BEST AVAILABLE COPY

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑪ 公開特許公報(A) 平2-110491

⑫ Int. Cl.⁵

識別記号

庁内整理番号

⑬ 公開 平成2年(1990)4月23日

G 09 C 1/10
G 06 F 12/14

3 2 0 B

7368-5B
7737-5B

審査請求 未請求 請求項の数 2 (全4頁)

⑭ 発明の名称 記憶装置

⑮ 特 願 昭63-264940

⑯ 出 願 昭63(1988)10月19日

⑰ 発 明 者 宮 口 庄 司 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

⑱ 発 明 者 岩 田 雅 彦 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

⑲ 出 願 人 日本電信電話株式会社 東京都千代田区内幸町1丁目1番6号

⑳ 代 理 人 弁理士 草 野 卓

明 細 書

1. 発明の名称

記憶装置

2. 特許請求の範囲

(1) 記憶媒体FDIに対し読み書きを行う記憶装置において、

上記記憶媒体FDIは識別名称FDIを有し、

鍵KIを生成する鍵生成手段と、

その鍵KIにより上記記憶媒体FDI内のデータを暗号化および復号化する暗号処理部とを備え、
上記鍵生成手段は

$KI = F(S, FDI)$

Fは鍵生成手段の処理を遂行するアルゴリズム、SはPの秘密パラメータ、により鍵KIを決めるものであることを特徴とする記憶装置。

(2) 上記記憶媒体FDIは保護コードFCIをも有し、
鍵生成手段の処理を遂行するアルゴリズムは $KI = F(SGI, FDI)$ 、但し $SGI = f(S, FCI)$ 、fはPの内部関数であることを特徴とする請求項1記載の記憶装置。

3. 発明の詳細な説明

「産業上の利用分野」

この発明は、記憶媒体の内容を暗号化及び復号化する機能を有する記憶装置に関するものである。

「従来の技術」

従来における記憶媒体FDの暗号化処理の決定方法は、次の通りである。

例1：全て同じ鍵を使う。この方法は鍵が一旦漏人に知られると全ての記憶媒体FDの内容が復号化されてしまうという欠点がある。

例2：各FD毎に異なる鍵列を使う。個別鍵は、鍵管理部を作って管理する。

この方法では、記憶装置は記憶媒体FDの個数だけ鍵を保有する必要があるため、記憶媒体FD数の増加と共に鍵の管理コストが大きくなる欠点がある。

この発明の目的は、鍵管理部を使わずに各記憶媒体FD毎に異なる個別鍵を使用し、記憶媒体FDの内容を暗号化及び復号化する機能を有する記憶装置を提供することにある。

特開平2-110491 (2)

「課題を解決するための手段」

記憶装置は、記憶媒体ドライブFD0と装置制御部とから成る。情報を記憶する記憶媒体FD0は、記憶媒体ドライブFD0に着脱可能または固定である。複数の記憶媒体FD0をFD1、1=1,2,...、で表す。各FDiは、その識別名称IDiと保護コードCiを持ち、IDiとCiをその内部に記憶する。IDiとCiは、暗号化と復号化の対象としない。

記憶媒体FD0に記憶するデータ(IDiとCiを除く)を暗号化及び復号化する鍵Kiは、次の様に定める。

$$Ki = F(Ci, IDi)$$

$$\text{但し、} Si = f_i(S, Ci)$$

ここで、Fは記憶装置が有する鍵生成アルゴリズム、 f_i はFの内部関数、SはFの秘密パラメータである。SはFDi側に格納する。

(他の鍵決定方法)

上記の鍵決定方法で、保護コードCiを使わない鍵決定方法である。即ち、鍵は以下により決める。

$$Ki = F(S, IDi)$$

(アルゴリズムF(S, Xi)の作り方)

を出力する形式の関数である。上述した識別名称IDiをNビットずつのデータに分け、左から順にXi1, Xi2, ..., Xioとおき、 $Ro = Iio, Ro = S$ として、ハッシュ関数により順次計算し、最後に得られるRoを、アルゴリズムF(S, Xi)の出力とする。

Fの内部関数fは、例えば $f_i(S, Ci) = S \oplus Ci$ 、或は、 $f_i(S, Ci) = (S \oplus Ci) \oplus q$ (qはビット対応の恒等論理和、Iはデータの連結、qは秘密の定数)として決めるが、内部関数fはSとCiの関数であれば適当に決めて良い。

「実施例」

第1図により説明する。記憶装置1は装置制御部2、記憶媒体ドライブ5a-1、5a-2から成る。装置制御部2は、内部にS保持手段、物理保護手段、鍵生成手段4a、暗号処理部3aを有する。記憶媒体ドライブ5a-1(1-1, 2)には、記憶媒体6a-1(1-1, 2)が着脱可能または固定である(第1図は記憶媒体を記憶媒体ドライブに装着した図である)。ホストコンピュータ7は、記憶装置1とデータの授受

第一の方法は、暗号化アルゴリズムEを用いてアルゴリズムFを作る方法である。Fは、次のように定める。

$$F(S, x_i) = E(S, x_i)$$

即ち、アルゴリズムFの秘密のパラメータSを鍵として、識別名称IDiを平文データと見なして暗号化する。ここでE(E, P)は鍵をEとしてPを平文データとして暗号化した暗号文を返す。識別名称IDiが長い場合は、識別名称IDiをNビットずつのデータのデータに分けてCBCモードで暗号化し、最後に得られる暗号文ブロックCoを、F(S, xi)の出力とする(CBCモードは国際規格ISO9317により定義される)。

第二の方法は、ハッシュ関数を用いてアルゴリズムを作る方法である。ここでハッシュ関数は以下に述べるものである。

$$Ro = f(Ro, Ro-1), u=1, 2, \dots, n$$

$$Ro: \text{データブロック}, Ro-1: \text{初期値(零など)}$$

ここで、RoやRo-1は、Nビットの長さがある。fは、RoとRo-1を入力変数とし、Nビット長データ

を行う。

S保持手段は、例えばバッテリバックアップによりパラメータSを常時メモリに記憶したおく。物理保護手段は、例えば物理鎖を付加することによりパラメータSの投入を制限し、またSを外側に露み出せない性質を持たせる。鍵生成手段4aは、パラメータSをS保持手段から入力し、識別名称IDiと保護コードCiを記憶媒体FDiから入力し、鍵Kiを生成し、この結果を暗号処理部3aに伝える。暗号処理部3aは、鍵生成手段4aから鍵Kiを受け取り、対象とするデータを暗号化または復号化する。

この記憶装置を動作させるためには、まず、鍵として物理鎖を所有するシステム管理者がS保持手段に秘密パラメータSを入力しておく。次に、暗号化及び復号化により以下の手順に従う。

(暗号化の場合)

ホストコンピュータ7からのデータを記憶すべき記憶媒体FD1、6a-1を記憶媒体ドライブ5a-1に装着する(FD1が記憶媒体ドライブに固定されている場合は除く)。装置制御部2は記憶媒体FD1、

特開平2-110491 (3)

6a-i 中の識別名称 IDi と保護コード Gi を読み取り、暗生成手段 4a 内の暗生成アルゴリズム P と S 保持手段内に保持しているパラメータ S を用い、

$$Ki = P(SGi, IDi)$$

$$\text{但し、} SGi = Ex(S, Gi)$$

により暗 Ki を決め、得られた Ki を用いてホストコンピュータ 7 からのデータ M を暗号処理部 3a により、

$$C = E(Ki, M)$$

と暗号化して記憶媒体 FDi、6a-i に記憶する。ここで、E(k, m) は、暗号処理部 3a が有する暗号化アルゴリズムであり、k は暗号化の鍵、m は平文データとする。

(復号化の場合)

記憶媒体 FDi、6a-i 内のデータを復号化して読み出す場合、まず、記憶媒体 FDi、6a-i を記憶媒体ドライブ 5a-j に装着する (FDi が記憶媒体ドライブに固定されている場合は除く)。装置制御部 2 は、記憶媒体 FDi、6a-i 中の識別名称 IDi と保護コード Gi を読み取り、暗生成手段 4a 内の暗生

成アルゴリズム P と S 保持手段内に保持しているパラメータ S を用い、

$$Ki = P(SGi, IDi)$$

$$\text{但し、} SGi = Ex(S, Gi)$$

により暗 Ki を決め、得られた Ki をもちいて記憶媒体 FDi、6a-i 内のデータ C を暗号処理部 3a により、

$$M = E^{-1}(Ki, C)$$

と復号化してホストコンピュータ 7 へ転送する。ここで $E^{-1}(k, c)$ は、暗号処理部 3a が有する復号化アルゴリズムであり、k は復号化の鍵、c は暗号文データとする。

「実施例 2」

実施例 1 において保護コード Gi を使わない方法である。即ち、

$$Ki = P(S, IDi)$$

により暗 Ki を生成する。他は実施例 1 と同様である。

「実施例 3」

図 2 図により説明する。パソコン 8 はパソコン主部 9、記憶媒体ドライブ 5b-1、5b-2 から成る。

パソコン主部 9 は内部に S 保持手段、暗生成手段 4b、暗号処理部 3b を有する。記憶媒体ドライブ 5b-j (j=1, 2) には、記憶媒体 6b-i (i=1, 2) が取脱可能または固定である (図 2 図は記憶媒体を記憶媒体ドライブに装着した図である)。

S 保持手段は、パラメータ S をメモリに記憶しておく。暗生成手段 4b は、パラメータ S を S 保持手段から入力し、識別名称 IDi と保護コード Gi を記憶媒体 FDi、6b-i から入力し、暗 Ki を生成し、この結果を暗号処理部 3b に伝える。暗号処理部 3b は、暗生成手段 4b から暗 Ki を受け取り、対象とするデータを暗号化または復号化する。

この記憶装置を動作させるためには、まず、利用者が、各利用者ごとに秘密のパラメータ S を入力し、これを S 保持手段に保持する。次に、暗号化及び復号化により以下の手順に使う。

(暗号化の場合)

パソコン 8 上のデータを記憶すべき記憶媒体 FDi、6b-i を記憶媒体ドライブ 5b-j に装着する (FDi が記憶媒体ドライブに固定されている場合

は除く)。パソコン主部 9 は、記憶媒体 FDi、6b-i 中の識別名称 IDi と保護コード Gi を読み取り、暗生成手段 4b 内の暗生成アルゴリズム P と S 保持手段内に保持しているパラメータ S を用い、

$$Ki = P(SGi, IDi)$$

$$\text{但し、} SGi = Ex(S, Gi)$$

により暗 Ki を決め、得られた Ki を用いて記憶すべきデータ M を暗号処理部 3b により、

$$C = E(Ki, M)$$

と暗号化して記憶媒体 FDi、6b-i に記憶する。ここで、E(k, m) は、暗号処理部 3b が有する暗号化アルゴリズムであり、k は暗号化の鍵、m は平文データとする。

(復号化の場合)

記憶媒体 FDi、6b-i 内のデータを復号化して読み出す場合、まず、記憶媒体 FDi、6b-i を記憶媒体ドライブ 5b-j に装着する (FDi が記憶媒体ドライブに固定されている場合は除く)。パソコン主部 9 は、記憶媒体 FDi、6b-i 中の識別名称 IDi と保護コード Gi を読み取り、暗生成手段 4b 内の暗

特開平2-110491 (4)

生成アルゴリズムFとS保持手段内に保持しているパラメータSを用い、

に基づき記憶装置の第3の実施例のブロック図である。

$$K1 = F(SG1, 1B1)$$

$$\text{但し、} SG1 = f_x(S, C1)$$

により鍵K1を決め、得られたK1を用いて記憶媒体

FD1、6b-1内のデータCを暗号処理部3bにより、

$$M = E^{-1}(K1, C)$$

と復号化してパソコン主部9へ転送する。ここで、

$E^{-1}(K, C)$ は、暗号処理手段3bが有する復号化アルゴリズムであり、Kは復号化の鍵、Cは暗号文データとする。

「発明の效果」

この発明による記憶装置は、記憶媒体FD1に異なる鍵K1が使えるので、一つの鍵K1が第三者に知られても、別の鍵K1がK1から算出できず安全性が高い。しかも、個別鍵を保持する鍵ファイルは不要で、鍵管理が簡単である。

4. 図面の簡単な説明

第1図は、この発明に基づく記憶装置の第1、

第2の実施例のブロック図、第3図は、この発明

特許出願人 日本電信電話株式会社
代理人 草野 卓

